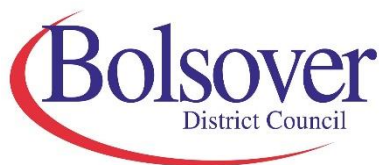


Public Document Pack



**North East
Derbyshire**
District Council

SUPPLEMENTARY AGENDA

Contact: Alan Maher
Tel: 01246 217391
Email: alan.maher@ne-derbyshire.gov.uk
Date: Thursday, 21 May 2020

To: **Members of the Joint ICT Committee**

Please attend a meeting of the Joint ICT Committee to be held on **Monday, 1 June 2020 at 2.00 pm** by conference call. Details will be sent to Committee Members separately.

Please note that the meeting will be live streamed on the North East Derbyshire District Council website.

Yours sincerely

A handwritten signature in black ink that reads 'Sarah Skerberg'.

Joint Head of Corporate Governance and Monitoring Officer

<u>Members of the Committee</u>	
Councillor J Lilley Councillor K Tait Councillor N Whitehead Councillor S Fritchley Councillor R Heffer Councillor D Salt Councillor C Furness Councillor D Hughes Councillor G Purdy	North East Derbyshire District Council North East Derbyshire District Council North East Derbyshire District Council Bolsover District Council Bolsover District Council Bolsover District Council Derbyshire Dales District Council Derbyshire Dales District Council Derbyshire Dales District Council

For further information about this meeting please contact: Alan Maher 01246 217391

AGENDA

5 **Minutes of Last Meeting** (Pages 3 - 9)

To approve as a correct record and the Chair to sign the attached Minutes of the meeting held on 10 February 2020.

9 **Quarterly Service Report** (Pages 10 - 30)

Report of the Head of the Joint ICT Service Delivery Manager

10 **Video and Audio Conferencing Tools** (Pages 31 - 38)

Report of the Joint ICT Service Delivery Manager



North East
Derbyshire
District Council

***We speak
your language***

Polish

Mówimy Twoim językiem

French

Nous parlons votre langue

Spanish

***Hablamos su
idioma***

Slovak

***Rozprávame Vaším
jazykom***

Chinese

我们会说你的语言

If you require
this agenda in
large print

or another
format
please call
us on

**01246
217753**

If you require an adjustment to enable you to participate in or access the meeting please contact the Governance Team at least 72 hours before the meeting starts.

JOINT ICT COMMITTEE

(Bolsover District Council, Derbyshire Dales District Council and North East Derbyshire District Council)

Minutes of the Meeting of the Joint ICT Committee held in the Council Chamber, District Council Offices, 2013 Mill Lane, Wingerworth, Chesterfield S42 6NG on 10 February 2020 at 10.00 am

Present:

Bolsover District Council (BDC)

Councillor R Heffer

Derbyshire Dales District Council (DDDC)

Councillor C Furness

Councillor D Hughes

Councillor G Purdy

North East Derbyshire District Council (NEDDC)

Councillor J Lilley

Councillor K Tait

Councillor N Whitehead

Officers:

Karen Henriksen – Head of Resources (DDDC)

Nick Blaney – Joint ICT Manager (NEDDC & BDC)

Matt Broughton – Joint Head of Partnerships and Transformation (NEDDC & BDC)

Nicola Astle – Joint ICT Infrastructure Manager (NEDDC & BDC)

Alan Maher – Senior Governance Officer (NEDDC)

Martin Derbyshire – Members ICT and Training Officer (NEDDC & BDC)

Tom Scott – Temporary Governance Officer (NEDDC & BDC)

30/19-20 Apologies for Absence

Apologies for absence were received from Councillor S Fritchley (BDC).

31/19-20 Declarations of Interest

There were no declarations of interest submitted for this meeting.

32/19-20 Minutes of Last Meeting

RESOLVED – That the Minutes of the meeting of the Joint ICT Committee held on 4 November 2019 were approved as a true and accurate record.

33/19-20 ICT Service Restructure

Members received a presentation from the Joint Head of Partnerships and Transformation on the ICT Service Restructure.

The Joint Head of Partnerships and Transformation explained that the Joint ICT Manager would be leaving his post at the end of February 2020. Members thanked him for all of his help and hard work.

34/19-20 Quarterly Service Report

Joint ICT Committee considered the latest performance report of the Joint ICT Service. This covered the third quarter of the financial year from October 2019 to December 2019. The Joint ICT Manager delivered the report and explained updates for performance, budget, resource utilisation, key projects, security and ongoing development of the service.

Members asked if the 'Project Related Activities' graph showing usage above target on a number of occasions meant that there were more Project Related Activities than planned. The Joint ICT Infrastructure Manager explained that this meant a higher percentage of time being spent on projects.

Members referred to the performance of Rykneld Homes (table 2.1.3 titled 'Incidents resolved within SLA target time') appearing to have the best figures for incidents resolved, and asked why this was. The Joint Head of Partnerships and Transformation explained that Rykneld Homes had simpler ICT systems, due to having one single major ICT business system and e-mails being handled by a third party.

The Committee agreed to note the report.

35/19-20 Cyber Security Presentation

Members received a presentation from the Joint ICT Infrastructure Manager on Cyber Security.

The presentation informed Members on the following areas:

Threat actors – who and why? (cyber criminals, foreign intelligence services, hackers and employees)

Current threats – malware, spyware, viruses, ransomware, phishing, false websites and e-mail spoofs

More threats – password brute force, zero-day attacks and DDoS attacks

How we protect ourselves – gateway security, anti-virus, encryption, patching, system monitoring, penetration testing, secure system, password policies, awareness and training

Achievements – achieved ‘amber/green’ in the LGA self-assessment tool in August 2019 after getting ‘amber/amber’ in August 2018. Received ‘substantial assurance’ in January 2020 from a network and internal security audit

Statistics – 139,000 e-mails blocked a month, block 2,700 attempts to access the network a month

The Joint ICT Infrastructure Manager advised Members that she would circulate the presentation to them after the meeting.

The Joint ICT Infrastructure Manager explained that phishing and ransomware attacks were the ones recorded most.

Members asked what kind of safeguards there were built into the system to detect problems with the system. The Joint ICT Infrastructure Manager explained that web/e-mail proxies, anti-virus and firewalls were in place for this along with regular patching, although organisations had no way of knowing when zero-day attacks would occur.

Members asked if the system picks up code being changed. The Joint ICT Infrastructure Manager explained that Windows picks up filename changes via its Microsoft resource manager as may the anti-virus products being used.

Members asked for zero-day attacks to be explained in more detail. The Joint ICT Infrastructure Manager informed them that zero-day attacks were attacks on software with known vulnerabilities which had no patch in place to fix, and code could be written to trick users into letting them on the network. There was a case study from 2017 at Copeland Borough Council where they were hit with a zero-day attack and given three days to respond.

Members asked if the incident at Copeland Borough Council had resulted in that authority publishing a report about the reasoning. The Joint ICT Infrastructure Manager explained that Copeland were putting together business continuity processes which could then be drawn upon by the Joint ICT authorities for experience.

Members asked if there was an offline backup of the system. The Joint ICT Infrastructure Manager explained that backup software had recently been acquired and space was being cleared to store the data.

Members asked which anti-virus software was used and if there was a tender process. The Joint ICT Infrastructure Manager explained that the anti-virus software was one of the leading security products, and reviews were regularly completed to ensure cost and effectiveness.

Members enquired if there was something in place for routers/servers to detect phishing sites. The Joint ICT Infrastructure Manager explained that an internal and external cloud pre-filter was in place. She added that educating officers on phishing was an important part of the protection, and this would be detailed in the next agenda item.

Members asked if penetration testing was done externally and how much it cost. The Joint ICT Infrastructure Manager explained that testing was done internally on a monthly basis, and an external company were paid to come in and test it once a year. This cost approximately £3,000 per authority.

Members requested that the presentation be circulated to Members of all three authorities.

Members noted the presentation.

(Joint ICT Infrastructure Manager)

36/19-20 'Phishing' Proposal

The Joint ICT Infrastructure Manager presented a report to update Members on phishing attacks and gain approval to complete a cyber security phishing awareness exercise for all employees and Members. The report also recommended that all Councils consider a Business Continuity exercise based upon a ransomware attack.

As a training and awareness exercise, the ICT department wanted to complete a simulated phishing exercise. Similar exercises had been recently completed by nearby councils and the results had demonstrated the following:

- a) The need for awareness, as a large percentage of users clicked on the phishing e-mail and provided sensitive information.
- b) The exercise was a valuable training tool as subsequent phishing exercises showed a significant reduction in the number of users who clicked the links and provided sensitive information.

Members agreed that the proposed simulated phishing exercise seemed very beneficial.

Members asked if anything was in place to prevent phishing when Members were given Council iPads. The Joint ICT Infrastructure Manager explained that an Information Security Policy was in place, but part of it still relied on people not clicking phishing links, which is where this training would come in.

The recommendations in the report were moved by Councillor Nick Whitehead and seconded by Councillor Garry Purdy. Members unanimously agreed to approve the recommendations.

Members requested that the most senior officers in attendance from each authority should follow these recommendations through to ensure they get carried out.

(Head of Resources/Joint Head of Partnerships and Transformation/Joint ICT Infrastructure Manager)

37/19-20 Budget Report

The Joint ICT Manager presented a Budget report to Members. The report updated Members on the projected outturn for the 2019-20 Joint ICT budget and sought approval for use of anticipated underspend.

The report showed the quarter 3 outturn for the Joint ICT Budget which had a current underspend of £44,000. This was because:

Employee costs

- Underspend due to delays recruiting to vacant posts
- Staff purchase of additional annual leave
- Underspend on training budget due to external grant funded training opportunity

Transport

- No fuel charges as yet so anticipated will be on budget

Services

- Outstanding commitments for Q4. Anticipated will come in on budget

The Joint ICT Manager explained that table 1.2 in the report showed an income of £21,860 for 2019/20. This came from services provided to others outside the partnership.

The recommendations in the report were moved by Councillor Garry Purdy and seconded by Councillor David Hughes. Members unanimously agreed to approve the recommendations.

(Joint Head of Partnerships and Transformation)

38/19-20 Critical Project Outcomes Report

The Joint ICT Manager presented a report to update Members on the outcomes of key infrastructure projects undertaken in 2018 and 2019.

The report explained that in 2018, work commenced on a series of time critical projects on the infrastructure that underpinned the technologies in place to deliver ICT services to partners. The key projects were:

- Migration to Windows 10 across all PCs and laptops
- Migration of all 2008 Server instances to 2012/2016 across all Windows Server instances used to deploy business systems

- Migration of all SQL 2008 databases to supported versions for all Business systems that use this database management system (DBMS)
- Deployment for a new backup solution for all partners' data

The Joint ICT service initiated projects managed and controlled by the partners' Project and Programme Methodology (PPM) to deliver these areas. The outcomes were:

Windows 10

- 487 Ageing PCs and laptops were replaced
- 285 Existing PCs and laptops were upgraded
- Total cost of new devices was £94,847 against a budget of £156,750
- 472 days of effort spend on design, build and deployment against an initial estimate of 798 days

Server 2008 Migration

- 99 server instances upgraded
- Total cost was £31,914 against a budget of £39,125, including SQL Server costs
- 92 days of effort against a an initial estimate of 136 days

SQL 2008 Migration

- 234 SQL Database instances upgraded
- 101 days of effort against an initial estimate of 90 days

Backup solution replacement

- 23 days for implementation against 60 day estimate
- Total cost of £63,900 against original budget of £125,000

The report included a recommendation that Committee acknowledge the contribution of staff to the successful delivery of these time critical, complex and high risk projects.

Members felt this was a positive report where savings had been found and the partnership between the three authorities had allowed for single upgrades across all of the Councils. Members wished to place on record their thanks to all of the officers who had worked hard (sometimes out of hours) on these projects.

Members asked if staff providing external services was something that had been considered. The Joint Head of Partnerships and Transformation explained that the service was in the process of an infrastructure programme, so all resources were committed to that at the moment. Members agreed that providing external services at this moment in time would mean spreading resources too thinly.

Members referred to the budgets for this report being underspends and budgets in other agenda reports being overspends, and asked why there were such variations. The Joint Head of Partnerships and Transformation explained that

budget estimation was sometimes difficult due to staff changes and business application vendors.

Members wished to add two further statements to the recommendation in the report:

a) That the Committee acknowledges and appreciates the hard work and contributions of all staff involved.

b) That the systems put in place are done over a number of years.

The recommendation in the report and the additional two statements were moved by Councillor Ray Heffer and seconded by Councillor Chris Furness. Members unanimously agreed to approve the recommendation and statements.

(Joint Head of Partnerships and Transformation)

39/19-20 Urgent Business

There was no urgent business for the Joint ICT Committee to consider at this meeting.

40/19-20 Future Meetings

The Senior Governance Officer informed Members that because the draft programme of meetings was not completed, he proposed meeting dates for the Committee on 11 May 2020 at Bolsover District Council and then another on 13 July 2020 at Derbyshire Dales District Council. He added that these dates would be confirmed with Members in the next month subject to availability.

(Senior Governance Officer)

Agenda Item 9

Quarterly Report on the Joint ICT Service (January 2020 to March 2020) OFFICIAL

1. Summary

It has been agreed that a quarterly report on Joint ICT Service will be provided to appraise the Joint Management Team and Shared Service Committee on performance, budget, resource utilisation, key projects, security and ongoing development of the service.

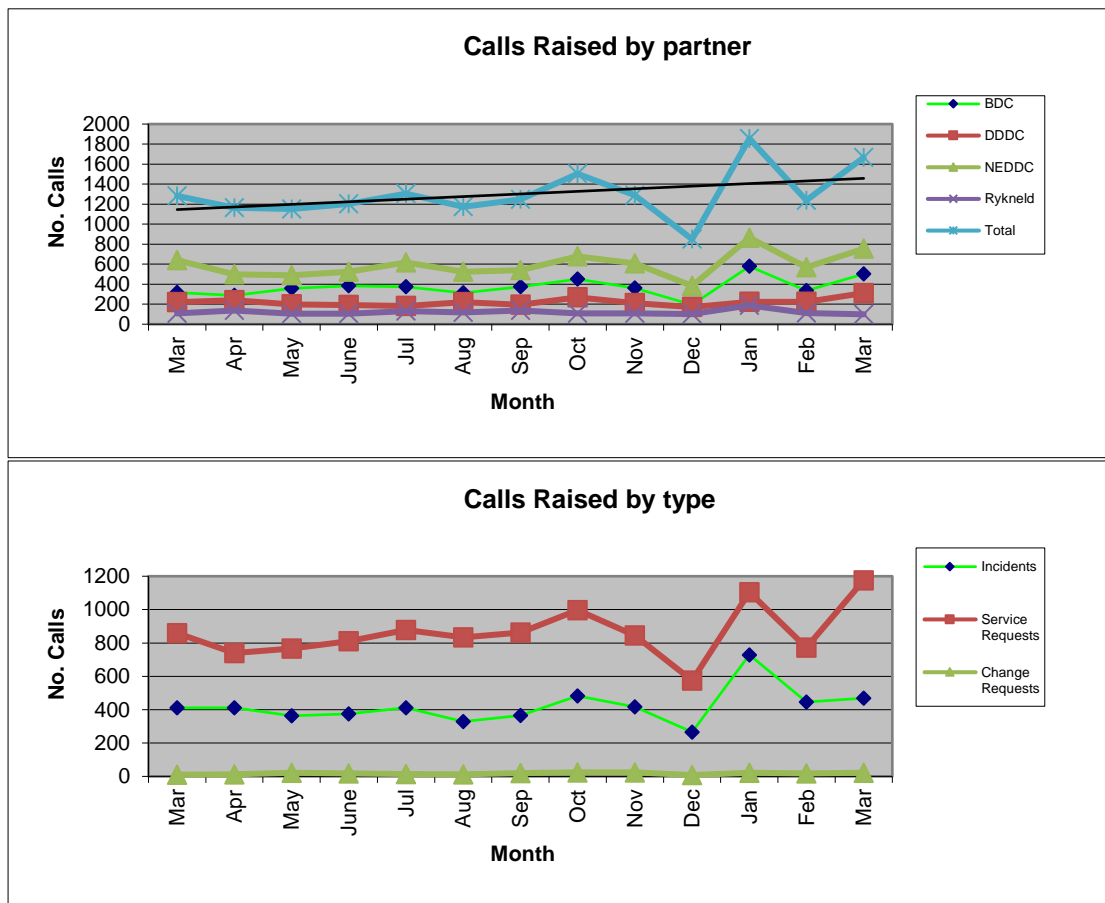
2. Performance

Background data and selected individual partner graphs that support the analysis below can be found in Appendix 1.

2.1 Support

The three Key Performance Indicators (KPI) as defined in the Service Level Agreements (SLA) between the Joint ICT Service and its partners are detailed below. Rykneld Homes are included for completeness although they have no formal involvement in the partnership, an SLA service is provided to them on behalf of North East Derbyshire District Council.

2.1.1 Calls



Quarterly Report on the Joint ICT Service (January 2020 to March 2020)

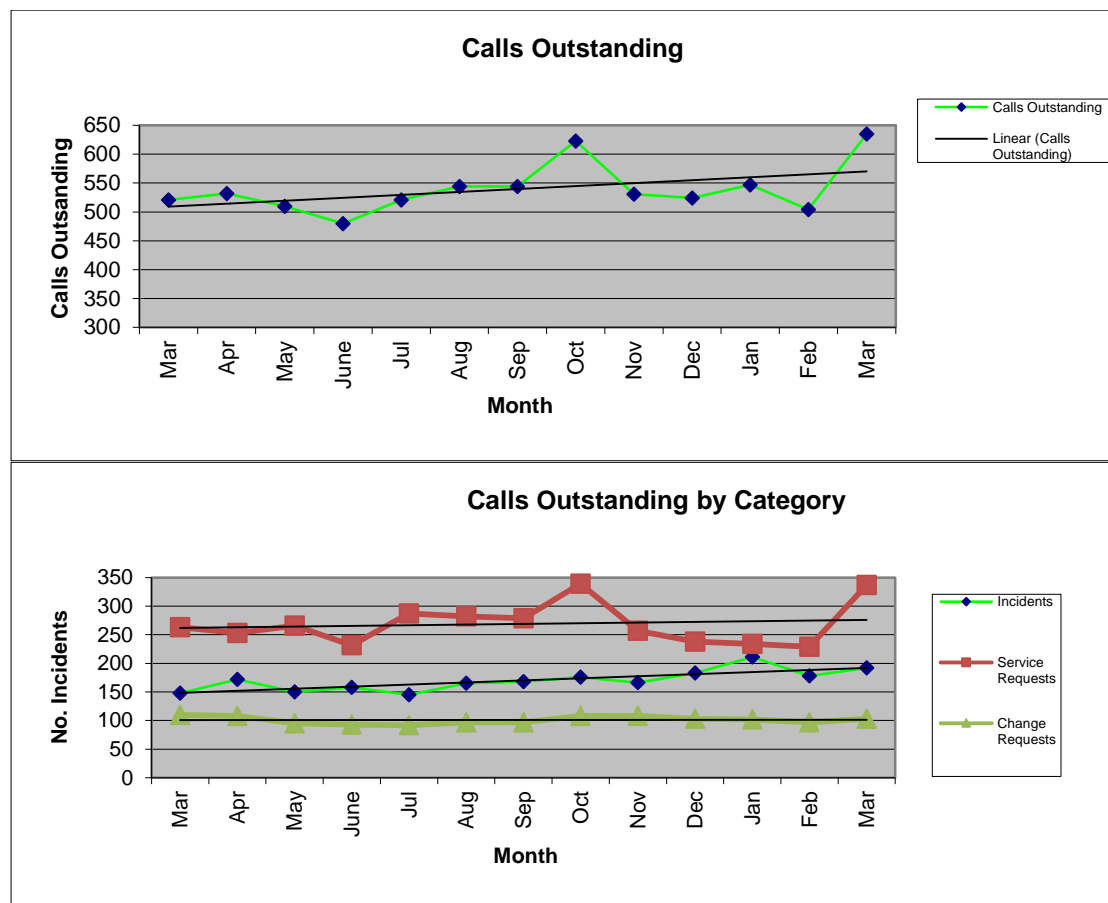
OFFICIAL

Whilst not a performance indicator in itself it does indicate the level of demand on the Service Desk.

Key points to note are:

- The total number of incidents and service requests raised was high throughout quarter four with January seeing the highest combined total of incidents and service requests being raised over the past 12 months, with March having the second highest.
- This increase was partly due to major upgrades to servers and virtual desktops (January/February) and additional requests due to the corona virus lockdown and facilitation of remote working (March).

2.1.2 Calls Outstanding



Again whilst not a performance indicator in the levels of outstanding calls gives an indication of potential future issues with the SLA Resolution performance indicator, project work and the impacts of staff absence on the service.

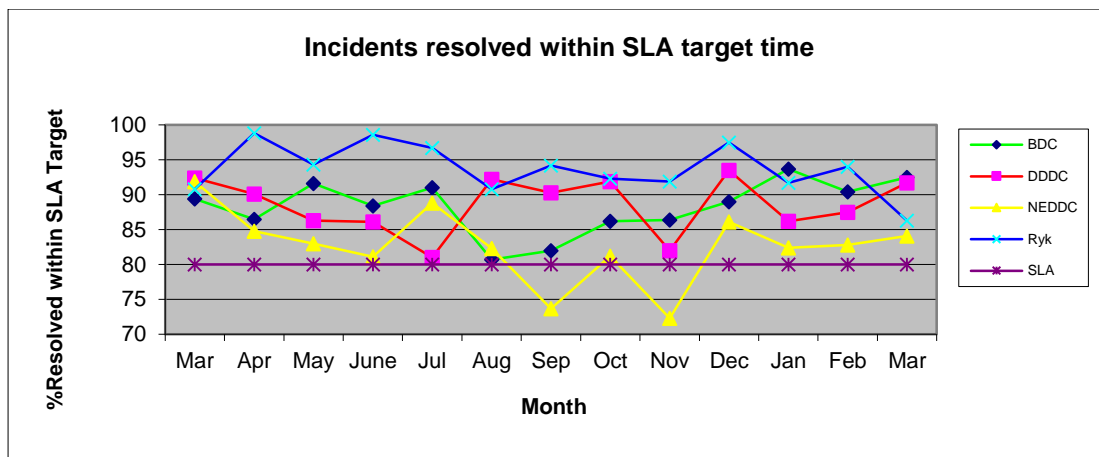
Key points to note are:

Quarterly Report on the Joint ICT Service (January 2020 to March 2020)

OFFICIAL

- Total number of outstanding calls increased instead of the anticipated decrease whilst focus was diverted to home working requests as a result of corona virus business continuity.
- This may rise again over the next quarter due to focus on Corona virus related activities and staff taking leave which was postponed to meet January operating system deadlines.

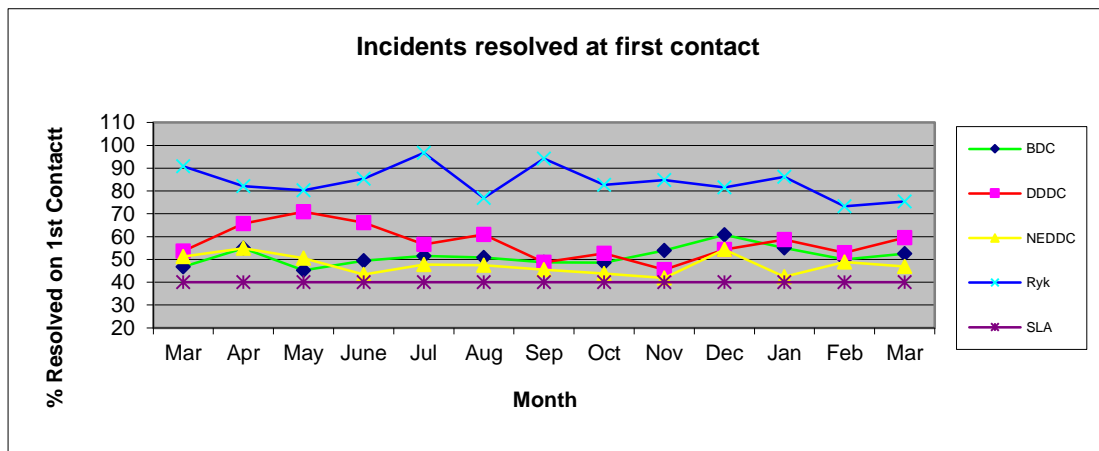
2.1.3 Incidents resolved within SLA Target time



Key points to note:

- No Breaches in the last quarter.
- Next quarter may result in breaches due to increased workloads and working from home due to Corona virus and business continuity activities.

2.1.4 Incidents resolved on 1st Contact



Points to note:

- No breaches in last quarter

**Quarterly Report on the Joint ICT Service
(January 2020 to March 2020)
OFFICIAL**

2.1.5 Outages

The service categories two types of major outage:

A priority 1 incident either affects a service delivered to customers or is impact staff across a number of service areas.

A priority 2 incident affects multiple users of a single system or service area.

In both cases staff are assigned to work on the incident immediately and ICT management are informed automatically.

Following any major incident a report is prepared which includes a root cause analysis, lessons learned and recommendations where applicable.

For this quarter the breakdown of incidents was as follows:

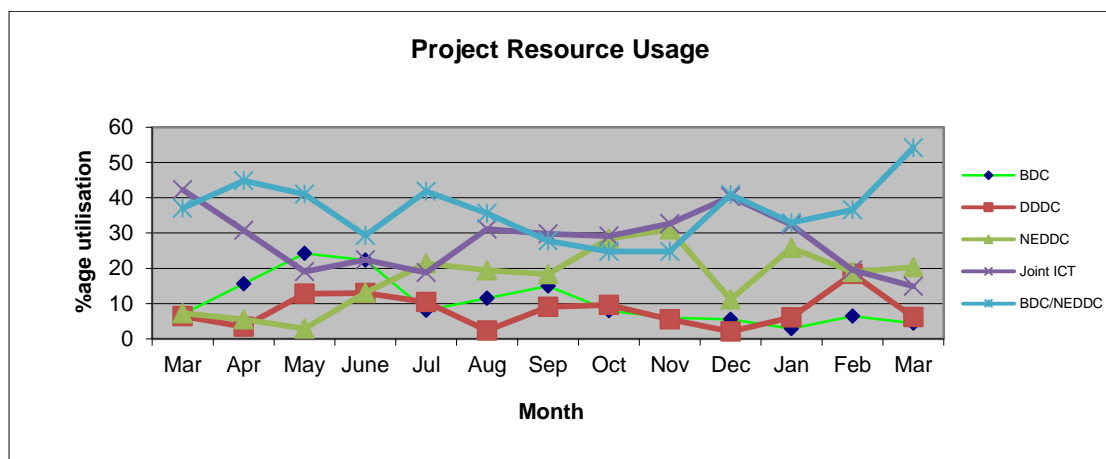
	January	February	March	Total
Priority 1	0	0	0	0
Priority 2	14	13	3	30
Total	14	13	3	30

There were no priority 1 incidents in the quarter

Priority 2 Incidents higher than usual in Jan and Feb due to several significant changes to the live environment.

2.2 Resource utilisation

As part of the SLA for the Joint ICT Service utilisation of resource for project related activities are monitored.

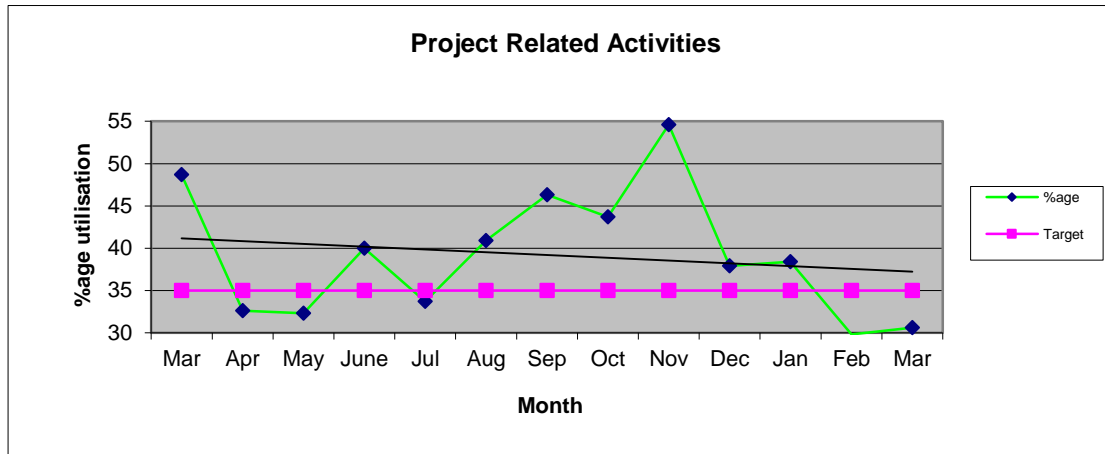


Key points to note are:

**Quarterly Report on the Joint ICT Service
(January 2020 to March 2020)
OFFICIAL**

- BDC/NEDDC Project times are high partially due to MFD rollout and business development work.

As a measure of how much time is spent on project related work within the Business Development and Infrastructure teams the following graph is provided:



Several projects came to an end in January with people subsequently taking leave. Focus moved to resolving large number of incidents and Corona virus related tasks during March.

2.3 Projects

Summarised below are the key projects underway or scheduled to start in coming three months and their status. Some projects have been put on hold as resources have been diverted to Corona virus / business continuity related activities.

2.2.1 BDC

OpenHousing

- Work progressing. User training in progress via video conference. Phase 1 implementation now moved to September 2020.

2.2.2 Derbyshire Dales

Electronic Document Management System

- Tactical deployments progressing

Meritec CRM

- Live April 2020 – further work on next phase

SIDD Replacement

- In progress

Capita SCP Payment portal / Paye.net

- Now live

2.2.3 NEDDC

**Quarterly Report on the Joint ICT Service
(January 2020 to March 2020)
OFFICIAL**

Leisure Dimension Upgrade

- Completed January

Rykneld Micollab

- On Hold due to Corona Virus

Missed bins reporting

- Complete

2.2.4 Strategic Alliance

Exchange Migration

- Completed January

MITEL Multimedia Services / Webchat

- Data Impact Assessment being completed.

Sip migration

- tender process on hold corona virus

MFD Replacement –

- New devices installed – awaiting collection of old devices after lock down.

Complaints system rewrite

- In progress

Modern.Gov

- Now Live

PCI Compliance

- Mid call solution in test

2.2.5 Joint ICT Service

OpenVPN

- Replaces Always on Vpn - Implemented during Corona Virus to assist remote working

Mid-Term Video/Audio Conferencing

- Setup as a result of Corona Virus to assist remote working

Internet Link Upgrade

- awarded to Virgin media Ltd, awaiting installation dates

Idox PA Upgrades

- BDC, NEDDC and DDDC Complete.

2020-21 Infrastructure work programme (draft)

- Office 365 discovery –in progress
- Phishing Exercise – on hold
- Active Directory Review –on hold
- Corporate Browser replacement.- 70% complete.

**Quarterly Report on the Joint ICT Service
(January 2020 to March 2020)
OFFICIAL**

- Cyber Security / PSN - ongoing
- Wi-fi refresh – in progress
- Symantec EV decommission – In progress
- Mid-Term Video Conferencing – In progress
- Switch replacement

The full project register can be seen in Appendix 2.

3.1 Joint ICT Service Budget – Q4 out turn (Period 1-12)

2019-20 Periods 1-12

Group		Full Budget	Budget YTD	Actual YTD	Variance
1****	Employees	1088784	1088784	1074727	-14057
3****	Transport	6310	6310	6970	660
4***	Services	86890	86890	78318	-8572
8***	Depreciation	1730	1730	1728	-2
9***	Income	-24909	-24909	-22614	2295
Y/E Finance adjustments					
Total		1158805	1158805	1139129	-19676

Variations(>£1,000):

- Employee costs
 - Underspend due to delays recruiting to vacant posts.
 - Staff purchase of additional annual leave
 - Training funded by LGA Cyber security Grant.
 - Additional termination costs due to restructure have been deducted.
- Services
 - Underspend on General expenses and Computer equipment.
- Income
 - Variable overtime re-charges

The additional termination costs due to the restructure have been deducted from the budget and the final outturn was an underspend of -£19,676.

This underspend can be either deducted from Q1 charges this financial year or retained to be used to re-invest in the service, details on any re-investment opportunities to follow before budget was re-allocated.

E.g. Cost associated with overlapping the increased internet bandwidth.

**Quarterly Report on the Joint ICT Service
(January 2020 to March 2020)
OFFICIAL**

4. Cost Saving Plan

Currently investigating moving NEDDC telephony to 'SIP' (Internet telephony) which will provide savings.

Tender completed for new joint Internet connection will deliver cost savings of £4000 per year and improved internet bandwidth although not until September 2021 and will result in additional costs during overlap.

The new multi-functional device contract will deliver savings of £13,000 per annum for BDC and £9,600 for NEDDC whilst also providing increased coverage of devices.

Plan can be seen in Appendix 3

5. Risk Register

Register reviewed and refreshed in December.

See Appendix 4.

6. Security Report

The Joint ICT Service maintains a log of all security related incidents, the vast majority of these are low level such as forgotten passwords. Serious breaches of Security would require reporting to the National Cyber Security Centre. The breakdown of security incidents for this quarter can be seen below. None qualified as a 'serious' breach that required reporting.

Incident Classification	BDC	DDDC	NEDDC	RHL
Reportable breaches				
Non reportable breach	2		1	
Attempted hack				
Advice				
Virus				
False positive				
Theft of device				
Website vulnerability				
Reported application vulnerability	1	1	1	0
Total	3	1	2	0

2 Mobile phones and 1 iPad missing.

**Quarterly Report on the Joint ICT Service
(January 2020 to March 2020)
OFFICIAL**

Apache Tomcat vulnerability with Capita's self-service – patches applied.

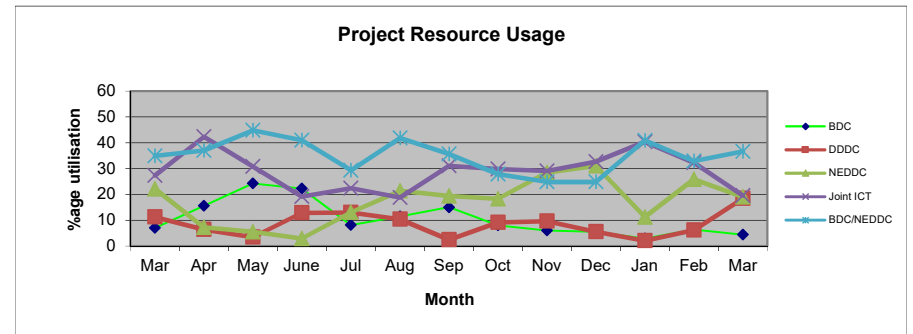
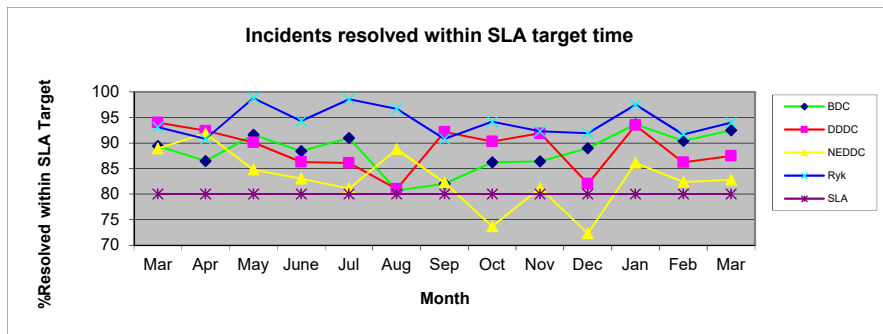
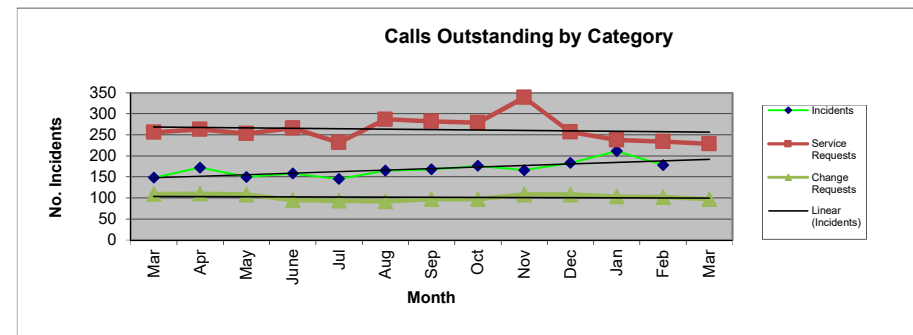
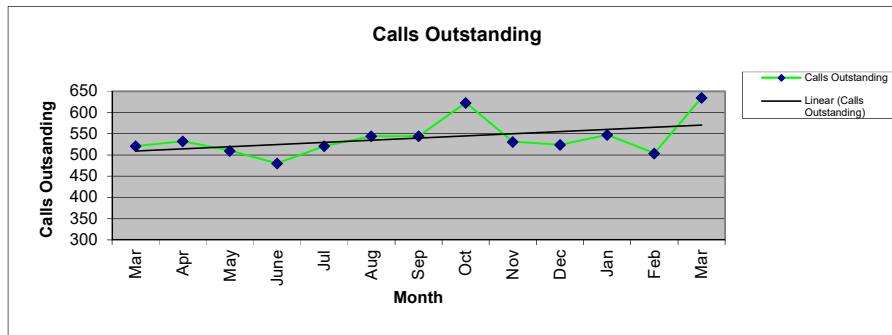
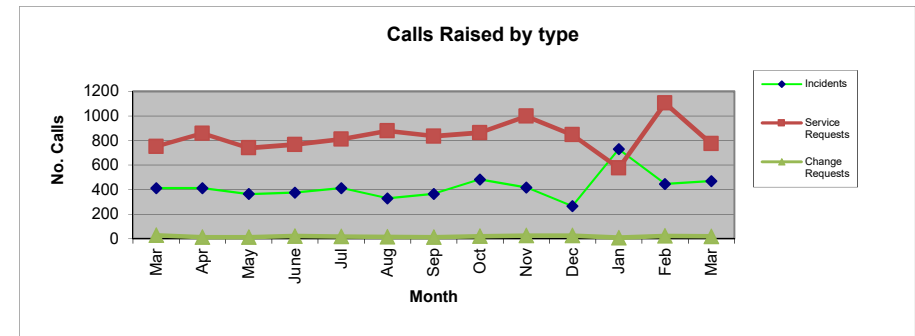
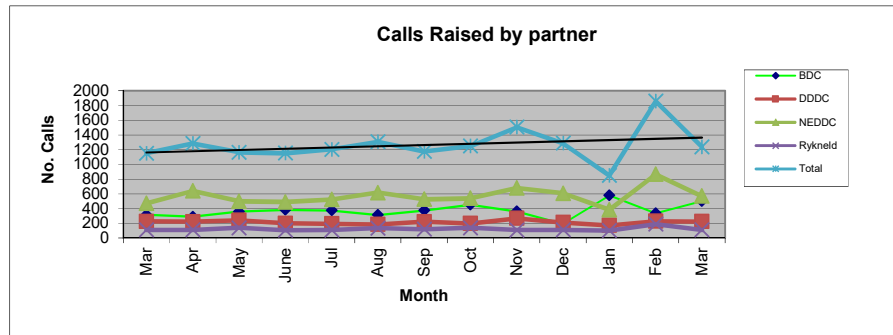
7. Service Development

New service restructure implemented as of 1st March.

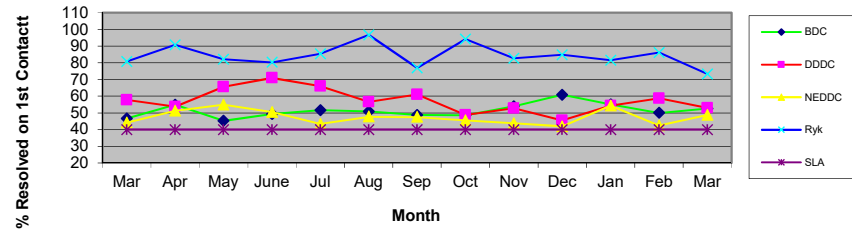
Senior Technology post recruited internally February.

Secured £5000 funding for each authority from LGA for cyber security resilience.

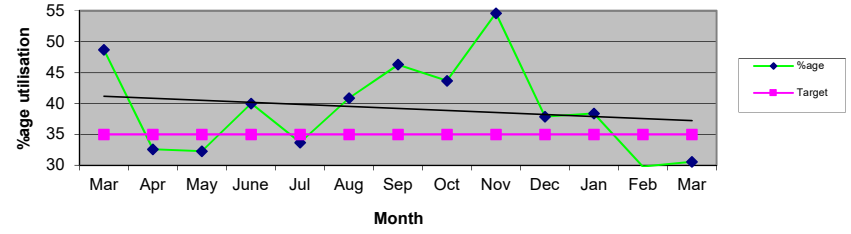
Secured funding for places on approved CISSP security training course for two members of ICT staff.



Incidents resolved at first contact



Project Related Activities



Joint ICT programme of work 2019

Ref	Project / Scheme	Project Stage	Update	Date of last update	RAG Status	Proj Spon	Proj Man	Team	Budget	Spend to date	Target Start/ Restart	Target End	BDT and Infrastructure Resource				
Start date 01/04/2018													Orig Est	Rev Est	Act Days	% Comp	Rem Days
1. Bolsover																	
BD18_01	Capita OPENHousing	2 - implementing	Datacut 5 complete. Live date 10 August 2020, delayed at Capita's request due to data issues. May be delayed until September 14th now due to delay in User Acceptance Testing because of CoranaVirus.	19/05/20	Amber	GG	DA	IN	£500k		1/4/18	10/8/20	40.0	110.0	108.0	98%	2.0
BD18_05	DEMS Bodycam System	4 - closed	Project Closed	04/02/20	Amber	PC	SW	IN			1/6/18	31/7/18	5.0	15.0	16.1	107%	-1.1
BDCB	Change requests 2019-20 - Business Development	4 - closed	Closed, new estimates for 20-21 based on this years actual	22/05/20	Green	KOG	KOG	BD			1/4/29	31/3/20	20.0	36.0	35.0	97%	1.0
BDCI	Change requests 2019-20 - Infrastructure	4 - closed	Closed, new estimates for 20-21 based on this years actual	22/05/20	Green	NA	NA	IN			1/4/19	31/3/20	40.0		10.7	27%	29.3
BD20_01	Change requests 2020-21 - Infrastructure	2 - implementing		01/04/20	Green	NA	NA	IN			1/4/20	31/3/21	13.0			0%	13.0
BD20_02	Change requests 2020-21 - Projects and Development	2 - implementing		01/04/20	Green	KOG	KOG	PD			1/4/20	31/3/21	38.0			0%	38.0
2. Derbyshire Dales																	
DD11a	EDRMS	2 - implementing	Minimal ICT input. Whilst not current focus some work is progressing with Legal and in relation to implementation of new Assure system across EH and licensing	02/01/20	Amber	SC	NA	IN			1/6/17	31/3/19	5.0	15.0	8.2	55%	6.8
DD18_04	Server 2008 Upgrades	4 - closed	Project complete	20/01/20	Amber	NA	NA	IN			1/6/18	31/12/19	47.0		37.1	79%	9.9
DD18_07	email retention policy	4 - closed	Project closed	14/02/20	Amber	K. Henriksen	NB	IN			1/6/18	2/1/19	20.0	11.7	10.2	87%	1.5
DD18_08	Customer Innovation Hub	4 - closed	Closed	30/01/20	Green	S. Lamb	KOG	BD			1/9/18	30/6/19	20.0		3.8	19%	16.2
DD19_01	Capita SCP Payment Portal	1 - Scope & Business Case	UAT complete, IB to clarify with Accountancy prior to final sign off.	09/01/20	Amber	S. Lamb	NA	IN			1/4/19	31/7/19	20.0		0.0	0%	20.0
DD19_05	Meritec Relationship Management	2 - implementing	22/5 Mertic go live was on schedule. Phase 2 commencing (Whitespace), CRM integration due by end July. Payment integrations in place. Estimates and end date increased to match phase 2 plan.	22/05/20	Green	PW	KOG	IN/BD			1/4/19	3/8/20	25.0		18.6	74%	6.4

Page 22

Ref	Project / Scheme	Project Stage	Update	Date of last update	RAG Status	Proj Spon	Proj Man	Team	Budget	Spend to date	Target Start/ Restart	Target End	BDT and Infrastructure Resource				
Start date 01/04/2018													Orig Est	Rev Est	Act Days	% Comp	Rem Days
DD19_06	SIDD Replacement	2 - implementing	Joomla! installed, along with utility plugins. Basic site structure created. Basic layout created.	30/01/20	Green	S. Lamb	BH	BD			4/12/19	22/7/20	55.0		21.8	40%	33.2
DD19_07	AgeUK Migration	1 - Scope & Business Case	On Hold - Corona Virus Awaiting Estates for relocation date	14.04.20	Amber	KH	NA	IN			4/12/19	30/1/20	5.0		1.1	22%	3.9
DD20_01	Capita Paye.net	2 - implementing	Test system installed 29/01/20. Testing period now commencing	30/01/20	Green	K.Henrik sen	SW	IN			19/12/19	13/4/20					
DD19_04	Change requests 2019-20 - Business Development	2 - implementing	Closed, new estimates for 20-21 based on this years actual	01/04/20	Green	KOG	KO	BD			1/4/19	31/3/20	20.0		4.9	25%	15.1
DD19_03	Change requests 2019-20 - Infrastructure	2 - implementing	Closed, new estimates for 20-21 based on this years actual	01/04/20	Green	NA	NA	IN			1/4/19	31/3/20	40.0		29.2	73%	10.8
DD20_03	Change requests 2019-20 - Business Development	2 - implementing		01/04/20	Green	KOG	KO	BD			1/4/20	31/3/21	7.0			0%	7.0
DD20_02	Change requests 2020-21 - Infrastructure	2 - implementing		01/04/20	Green	NA	NA	IN			1/4/20	31/3/21	32.0			0%	32.0
3. North East Derbyshire																	
NE18_04	Info@work Upgrade v5.11	4 - closed	Closure Approved	17/02/20	Red	NA	NA	IN			22/11/18	30/6/19	20.0		25.6	128%	-5.6
NE19_03	Website redesign	4 - closed	Closure approved	23/01/20	Green	MB	KOG	BD			1/6/19	31/12/19	60.0	70.0	72.9	104%	-2.9
NE19_04	Automated Site Assessment	4 - closed	Project closed	27/03/20	Red	RP	AC	BD			1/7/19	30/11/19	15.0	20.0	23.3	117%	-3.3
NE19_05	Chip&Pin Replacement	3 - awaiting closure report	All devices swapped and are live. loan devices returned	28/01/20	Amber	MB	PL	IN			23/7/19	31/12/19	7.0		1.1	16%	5.9
NE19_06	Leisure Dimensions Upgrade	2 - implementing	Dimensions now live, issues with new web portal being looked at by xnleisure.	30/01/20	Green	MB	RS	IN			8/8/19	31/1/20	7.0		6.0	86%	1.0
NE19_07	Missed Bins Reporting Online	4 - closed	Project Closed	05/05/20	Amber	SB/MB	KOG	BD			1/9/19	31/12/19	10.0	29.0	33.5	116%	-4.5
NE20_01	RHL MiCollab	1 - Scope & Business Case	Project brief required	20/02/20	Green	LG	SH	IN			6/2/20	15/4/20	66.0		0.2	0%	65.8
NECB	Change requests 2019-20 - Business Development	2 - implementing	Closed, new estimates for 20-21 based on this years actual	01/04/20	Green	KOG	KO	BD			1/4/19	31/3/20	10.0	20.0	35.8	179%	-15.8
NECI	Change requests 2019-20 - Infrastructure	2 - implementing	Closed, new estimates for 20-21 based on this years actual	01/04/20	Green	NA	NA	IN			1/4/19	31/3/20	40.0		25.8	65%	14.2

Ref	Project / Scheme	Project Stage	Update	Date of last update	RAG Status	Proj Spon	Proj Man	Team	Budget	Spend to date	Target Start/ Restart	Target End	BDT and Infrastructure Resource				
Start date 01/04/2018													Orig Est	Rev Est	Act Days	% Comp	Rem Days
NE20_02	Change Request 2020-21 - Infrastructure	2 - implementing		22/05/20	Green	NA	NA	IN			1/4/20	31/3/21	28.0			0%	28.0
NE20_03	Change Request 2020-21 - Projects and Development	2 - implementing		22/05/20	Green	MB	KOG	IN			1/4/20	31/3/21	38.0			0%	38.0
4. Joint service																	
J118_01	AlwaysOnVPN	5 - on hold	Replaced by OpenVPN project	on hold	Amber	NA	LT	IN			1/1/18	30/6/18	35.0		3.7	11%	31.3
J118_09	Apple Management	2 - implementing	Community Arts & Communications Complete. Staff & Member iPads in progress NE - Only 5 left to do in ICT. BDC - 2 left to do.	10/01/20	Amber	NA	MJR	SD			8/8/18	31/3/19	13.0	30.0	22.7	76%	7.3
J118_10	User Device Refresh 2018	4 - closed	Project Closed	20/01/20	Amber	NB	MJR	SD			1/9/18	31/12/19	555.0		58.5	11%	496.5
J118_11	Replacement Backup Storage	4 - closed	Project Closed	28/01/20	Green	NB	NA	IN			1/10/18	1/10/19	60.0	25.0	23.5	94%	1.5
J118_12	Website Vulnerability Review 18-19	2 - implementing	OLA now approved by all parties. NEDDC Joomla vulnerability now resolved. BDC Joomla vulnerability still present but now	20/05/20	Amber	NA	LT	IN/BD			31/10/18	31/10/19	43.0		1.1	3%	41.9
J118_13	Active Directory & GPO Review	1 - Scope & Business Case	New/updated PB required due to being on hold for so long. Scoping session, to establish scope. (19-05-20 - no progress due to coronavirus & related commitments - MTG)	19/05/20	Amber	NA	MG	IN			1/11/18	1/4/19	112.0		1.2	1%	110.8
J118_14	Windows 10 Upgrades	4 - closed	project Closed	20/01/20	Green	NA	MJR	SD			2/10/18	31/12/19	168.0	180.0	210.4	117%	-30.4
J119_02	Browser Replacement	2 - implementing	On Hold - COVID 19. Chrome as default in W10 VDI. Chrome and policies on physical PCs. Next stage to move sections of staff to Chrome as default.	19/05/20	Amber	NA	CP	IN			1/3/19	30/8/19	12.0		3.8	32%	8.2
J119_05	PSN Compliance 2019-2020	2 - implementing	DDDC PSN Code of Connection now passed. BDC November PC IT Health Check. Remediation. Neddc PSN submission delayed owing to Co-Vid. DDDC PC IT Health Check due to start in June 2020	20/05/20	Green	NA	LT	IN			1/2/19	31/3/20	136.0		58.2	43%	77.8
J119_06	Exchange 2016 Migration	3 - awaiting closure report	All three 2010 exchange servers migrated and decommissioned	20/02/20	Red	NA	NA	IN			1/9/19	28/2/20	37.0		0.9	2%	36.1

Ref	Project / Scheme	Project Stage	Update	Date of last update	RAG Status	Proj Spon	Proj Man	Team	Budget	Spend to date	Target Start/ Restart	Target End	BDT and Infrastructure Resource				
Page 24	Start date	01/04/2018											Orig Est	Rev Est	Act Days	% Comp	Rem Days
	J119_07	Office365 Discovery	1 - Scope & Business Case	Preliminary investigations established SA migration possible, required exchange 2016. Licence costs established for further discussions with Committee members.	09/01/20	Green		NA	IN						1.4		
	J120_01	New Internet Connection	1 - Scope & Business Case	Awaiting installation information from Virgin.	21/01/20	Green	NA	LT	IN		1/2/20	30/8/20					
	J120_02	Mobile Device Management	1 - Scope & Business Case	Business case being prepared	17/02/20	Green	NA	TB	IN								
	J120_03	VMWare ESXi Upgrades 2020	2 - implementing	Initially Delayed due to C19, ICT resource now permits working on this starting with DDDC W/C 25th May to support PCITHC Remediation - TAB	19/05/20	Green	NA	TB	IN		25/5/20	25/8/20	21.5				
	J119_03	Change Request 2019-20 - Infrastructure	2 - implementing		06/03/20	Green	NA	NA	IN		1/4/19	31/3/20	10.0	15.0	14.4	96%	0.6
	J119_04	Change Request 2019-20 - Business Development	2 - implementing		06/03/20	Green	MB	KOG	BD		1/4/19	31/3/20	20.0		2.3	12%	17.7
5. Strategic Alliance																	
SA22	PCI-DSS	1 - Scope & Business Case	Mid-call at BDC implementing. Testing due wc 19052020. NEDDC procuring Capita end call solution. Still awaiting XNPAY costs. Kiosk will be decommissioned on 31/12/19. Awaiting decision on Civica offer at BDC.	19/05/20	Amber	L. Hickin	NA	IN			1/7/17	31/3/20	5.0	20.0	26.2	131%	-6.2
SA16_06	Revenues Derbyshire Fraud Initiative and Digital Transformation	4 - closed	Project Closed	17/03/20	Red	DC	NA	IN			1/1/17	30/4/17	20.0	40.0	21.8	55%	18.2
SA18_03	Transformation programme work	2 - implementing	Digital Strategy approved by BDC, Exec at NED. Both Climate strategies approved. Leadership Academy projects commenced. Issues around project monitoring (timescales)	06/03/20	Green	LH	KOG	BD			19/3/18	31/3/22	40.0	120.0	48.7	41%	71.3

Ref	Project / Scheme	Project Stage	Update	Date of last update	RAG Status	Proj Spon	Proj Man	Team	Budget	Spend to date	Target Start/ Restart	Target End	BDT and Infrastructure Resource				
Start date 01/04/2018													Orig Est	Rev Est	Act Days	% Comp	Rem Days
SA18_04	Server 2008 Upgrades	4 - closed	Project complete	20/01/20	Red	NB	NA	IN			1/6/18	31/12/19	93.0		54.5	59%	38.5
SA18_08	Smartphone Upgrades	2 - implementing	In progress: BDC: 86% NEDDC: 80%	04/12/19	Amber	NA	MJR	SD			10/1/19	30/6/19	16.0		2.5	16%	13.5
SA19_03	Civica financials v19 upgrade and migration	4 - closed	Project Closed	11/02/20	Red	DC	PL	IN			15/2/19	31/5/19	15.0		16.4	109%	-1.4
SA19_07	MFD Contracts 2019	4 - closed	Project Closed	24/02/20	Green	MB	NB	IN			1/5/19	31/3/20	25.0	13.0	13.0	100%	0.0
SA19_08	Mitel Estate Upgrade	4 - closed	Project has a closure report - 20191209. Resilient DMZ MBG to be configured by 4sight - aim to be completed 16/01/2020	09/01/20	Red	NA	CP	IN			1/5/19	30/8/19	42.0		42.0	100%	0.0
SA19_10	Modern.gov	2 - implementing	19/5 live at NEDDC and BDC. Awaiting Calender integratin with Modern.gov	19/05/20	Green	NC	RS	IN/BD			17/7/19	1/3/20	11.5		15.2	132%	-3.7
SA19_13	Env Health User Account Rationalisation	2 - implementing	PB Approved. 20/42 Machines built and in use.	13/01/20	Amber	NA	HH	SD			13/12/18	28/2/20	17.0		4.0	24%	13.0
SA19_14	Complaints System Rewrite	2 - implementing	Progressing well since Jan	06/03/20	Green	MB	HB	BD			13/1/20	1/7/20	35.0		15.1	43%	19.9
SA20_01	SIP Migration	2 - implementing	Investigation with suppliers	30/01/20	Green	MB	NA	IN			1/1/20	31/3/20	11.0			0%	11.0
SA20_03	Moving in/out of the district	5 - on hold	Waiting to hear from NEDDC revenues - will the ieg4 or Capita form do the job instead?	20/02/20	Green			BD									
SA20_04	Webchat and Multimedia CCM	1 - Scope & Business Case	Project brief required	20/02/20	Green	MB	SH	IN									
SA20_05	Tranman 9 Upgrade	2 - implementing	PB needs approval	21/02/20	Green	SB	RS	IN			30/1/20	14/7/20	5.0			0%	5.0

Ref	Project / Scheme	Project Stage	Update	Date of last update	RAG Status	Proj Spon	Proj Man	Team	Budget	Spend to date	Target Start/ Restart	Target End	BDT and Infrastructure Resource					
Page 26	Start date 01/04/2018												Orig Est	Rev Est	Act Days	% Comp	Rem Days	
	SA20_06	Enterprise Vault Phase Out	1 - Scope & Business Case	PB to be approved	11/03/20	Green	MB	RS	IN			1/2/20	31/4/20	6.5			0%	6.5
	SA20_07	Kyocera MFD Deployment	2 - implementing	Kyocera devices deployed, but still using Konicas for Paris printing due to onsite testing and Coronavirus. Still awaiting Ricoh for NEDDC Print & Design and Konica collection of old devices.	19/05/20	Green	NA	DA	IN			10/2/20	31/3/20	20.0			80%	4.0
	SA19_06	Change requests 2019-20 - Business Development	2 - implementing		30/01/20	Green	NA	KOG	IN			1/4/19	31/3/20	45.0	120.0	109.9	92%	10.1
	SA19_05	Change requests 2019-20 - Infrastructure	2 - implementing		30/01/20	Green	MB	NA	IN			1/4/19	31/3/20	25.0		1.6	6%	23.4
Project Effort Distribution																		
BD	Q1	Q2	Q3	Q4	Total Days	2 people, 213 days each, 3.33 at 75% of time on projects, one at 50%(BDM)												
Days required	#VALUE!	#VALUE!	#VALUE!	#VALUE!	#VALUE!													
Availability	80	80	80	80	320													
Days Over/under comm	#VALUE!	#VALUE!	#VALUE!	#VALUE!	#VALUE!													
Cumulative over/under	#VALUE!	#VALUE!	#VALUE!	#VALUE!	#VALUE!													
GI	Q1	Q2	Q3	Q4	Total Days	2 people, 213 days, 2 x 50%												
Days required	0	0	0	0	0													
Availability	53	53	53	53	212													
Days Over/under comm	53	53	53	53	212													
Cumulative over/under	53	106	159	212														
IN						12 people, 213 days each, 30% of time on projects												
Days required	#VALUE!	#VALUE!	#VALUE!	#VALUE!	#VALUE!													
Availability	175	190	190	190	745													
days Over/Under	#VALUE!	#VALUE!	#VALUE!	#VALUE!	#VALUE!													
Cumulative over/under	#VALUE!	#VALUE!	#VALUE!	#VALUE!	#VALUE!													
Total(BD+GI+INF)																		
Total days needed	#VALUE!	#VALUE!	#VALUE!	#VALUE!	#VALUE!													
Availability	308	323	323	323	1277													
Days over/under	#VALUE!	#VALUE!	#VALUE!	#VALUE!	#VALUE!													
Cumulative over/under	#VALUE!	#VALUE!	#VALUE!	#VALUE!	#VALUE!							Calendar Days Remaining:						

Cost Saving Plan																		
			Potential savings:								Actual							
Activity	Start	End	DDDC	NEDDC	BDC	Joint	Saving	Year	Status	One off/Recurring	saving	Comment						
2019-20																		
PSN Connectivity aggregation	01/05/19	31/03/20	4,000	4,000	4,000		R	2020-21		R	8,000	part year, fully realised 20-21						
Joint Scanner Maintenance contract	01/09/19	31/08/20	275	340	1,030		R	2019-20		R	1,645							
New Mobile Device Contract	01/08/19	31/03/20		2,000	2,000		R	2020-21		R	4,000	part year, fully realised 20-21						
WAN resign	01/08/19	31/03/20		4,308			R	2020-21		R	4,308							
DDDC WAN contract	01/05/19	31/03/20	4,135				R	2020-21		R	4,135	part year, fully realised 20-21						
Take on UPS contracts for Arc and Rivers	01/10/19	30/09/20			3,400		R	2020-21		R	3,400							
			8,410	10,648	10,430	0					25,488							
2020-21																		
New MFD Contact	01/03/20	28/02/25		9,647	13,712		R	2019-20		R	23,359	based on usage for 2019						
SIP Migration	01/06/20	30/05/23					R	2020-21		R	0	awaiting budgetary quotations	part year, fully realised 21-22					
			0	9,647	13,712	0					23,359							
Saving Legend:																		
R - Retained budget																		
J - Joint ICT budget																		
A - Cost Avoidance																		
I - Income																		
X - Cost Increase																		
One off/Recurring																		
O - Recurring																		
R- Recurring																		

Joint ICT Service Area RISK REGISTER as at: 27th May 2020

Current Risks

Risk UID	Risk	Consequences	Gross Risk (Probability x Severity)	Mitigating Actions	Net Risk (Probability x Severity) Taking into Account Current Controls	Risk Owner
02	Increase in cost of the service	Pressure on partner budgets.	3 x 4 = 12	Savings realised by partners, strong governance in place. Sterling impact on licensing a concern.	2 x 4 = 8	Joint Management Team
03	A member of the partnership withdraws	Potential short term costs and increase in service costs	1 x 4 = 4	Exit Strategy drafted, strong governance in place. Benchmarking undertaken and value for money demonstrated.	1 x 4 = 4	Joint Management Team
04	Conflicting requirements for cost reductions	Reduction of SLA targets and withdrawal of aspects of the service	3 x 4 = 12	Annual budget review process in place	2 x 4 = 8	Joint Management Team
05	Uneven demands for resource	Partners gaining inequitable share of available resources	3 x 3 = 9	Project resource management and monitoring introduced and refined in 2014.	2 x 3 = 6	Join ICT Delivery Manager
06	Staff retention	High turnover of staff in a service can lead to drops in productivity and service levels	2 x 4 = 8	Current team has high morale and relatively low sickness rates. Low staff turnover rates.	2 x 4 = 8	Join ICT Delivery Manager
10	Insufficient capacity within service to meet business demands	Unable to delivery key projects for partners	5 x 3 = 15	Effective prioritisation by corporate management. Funding considered on a project by project basis. Additional resource proposed as part of 2019 service restructure	3 x 3 = 9	Joint Management Team

Joint ICT Service Area RISK REGISTER as at: 27th May 2020

11	Impact of long term sickness absences on service	Backlog of service requests and failure to meet KPI's. Conflict in resource demand for projects and changes	$5 \times 3 = 15$	Monitor workloads, raise awareness with user groups, joint management team and senior management as appropriate, reprioritise workloads, re allocate workload across teams. Manage expectations	$5 \times 2 = 10$	Joint Management Team
13	Impact on revenue budgets of currency fluctuations	A weakening of sterling results in increased revenue costs for our software license subscriptions and some hardware related costs as the vendors are US Dollar based organisations	$5 \times 3 = 15$	Where possible some procurements can be brought forward to avoid upcoming increases. Consideration for multiyear agreements to 'lock in' pricing may help in short term.	$5 \times 3 = 15$	Join ICT Delivery Manager

Closed or Mitigated Risks

Risk UID	Risk	Consequences	Gross Risk (Probability x Severity)	Mitigating Actions	Net Risk (Probability x Severity) Taking into Account Current Controls	Risk Owner
01	Anticipated cost savings not realised	Key benefit to partners not achieved.	$3 \times 5 = 15$	Savings delivered additional actions to be documented and monitored in a Cost Savings Plan	$1 \times 5 = 5$	Join ICT Delivery Manager
08	Loss of Pioneer House facility	ICT and DR services could not operate from this site	$2 \times 5 = 10$	Staff can work remotely and at partner sites. DR service loss for duration.	$1 \times 4 = 4$	Join ICT Delivery Manager
07	Comprehensive Spending Review/Grant Settlement	Unexpected reduction in funding would damage ability to deliver service at current levels	$3 \times 5 = 15$	Joint monitoring of performance, budget and risk	$2 \times 5 = 10$	Joint Management Team

Joint ICT Service Area RISK REGISTER as at: 27th May 2020

09	Failure to achieve PSN compliance	Loss of access to key systems for Benefits, electoral registration and contact centres teams	$2 \times 5 = 10$	Maintain priority within service and maintain resource levels	$1 \times 5 = 5$	Joint Management Team
12	Retention of apprenticeship schemes	If apprenticeships not maintained service KPI's will suffer and likely breach. On site staff coverage compromised	$5 \times 3 = 15$	Funding for full time roles for existing apprentices approved in 2019. Future apprenticeships will be offered when vacancies arise in Service Desk team.	$4 \times 2 = 8$	Join ICT Delivery Manager

Bolsover, Derbyshire Dales and East Derbyshire District Councils

Joint ICT Committee

1 June 2020

Video and Audio Conferencing Tools

Report of the Joint ICT Service Delivery Manager

Purpose of the Report

- To update Councillors on and background for issuing 'Members protocol for the use of video and audio conferencing' to join official council related meetings.
- To request Councillors support the guidance and acknowledge the risks associated with video conferencing.

Report Details

- 1.1. Since the outbreak of corona virus and the Government decision to invoke social distancing and lock-down, there became an urgent requirement for conferencing tools to enable groups of people to collaborate whilst geographically separated.
- 1.2. Numerous conferencing tools are available with no one tool being used consistently throughout partner organisations or the wider business community.
- 1.3. ICT are receiving numerous requests to JOIN meetings hosted by third parties using various collaboration technologies. The main ones being GoToMeeting, Zoom, Skype, Microsoft Teams and Cisco WebEx.
- 1.4. It is often essential that members and officers collaborate in these meetings and ICT want to assist and not to be a barrier to the use of essential collaboration technologies during this time.
- 1.5. However, each technology is different. They offer different functionalities such as file sharing, which pose different security risks with regards to loss of data and potential harm to the council's network. They can be recorded which could infringe on peoples data protection rights. They use different levels of encryption, and have differing privacy statements and are hosted in different countries.
- 1.6. The installation and use of these tools is not standard either, some will work via a web browser on a laptop, whilst iPads are required to be brought into the office for applications to be installed.
- 1.7. Being cloud based technologies, once access to these tools are provided we have very little technical controls that we can put in place to restrict how they are used or

by who. For example, we cannot restrict file sharing, or prevent users from signing up with their corporate email addresses.

- 1.8. The practical ways we can mitigate the risks whilst enabling virtual conferencing to support official council related business is to either prohibit their use or ask councillors and staff to agree to a protocol of usage which determines what they should and should not do whilst using the different collaboration tools.
- 1.9. The unmitigated cyber and data security risks are significant. See **Appendix 5 – Audio and Video Conferencing risk Register 28.04.20**
- 1.10. 'Members Protocols for the use of Video and audio conferencing have therefore been produced and distributed to all Members, in order to mitigate some of the risks associated with the use of these tools. Similar ones have been sent to staff.
- 1.11. If access to JOIN (NOT HOST) a meeting using GoToMeeting, Skype, Microsoft Teams, Zoom and Cisco WebEx is necessary for official Council business/meetings and the application is not available on corporately provided equipment, a call to the Member Support Officer (BDC&NEDDC) or Servicedesk (ALL) will be required so that the iPad can be updated.
- 1.12. The protocol also specifies that HOSTING of video conferencing on behalf of the Council should only be done via corporately purchased accounts, currently Governance and Democratic services have these.
- 1.13. Although not fully addressing all risks, through the Member and staff acceptance of the protocol, the authority can help to mitigate some of the risks associated with the use of the most commonly used video and audio tools where technical constraints are not available.
- 1.14. Video and audio conferencing technology is improving/maturing at a fast pace. The protocol should be reviewed regularly and is subject to change as new technologies and information becomes available and as requirements change.
- 1.15. It is envisaged that parts of the protocol will eventually be incorporated into the corporate ICT security policy once future corporate video and audio tools are reviewed and confirmed.

2. Internet Bandwidth and Video /audio conferencing

- 2.1. Video and audio conferencing is directly impacted by the network / internet connection being utilised. This could be wired or over Wi-Fi, via people's home broadband / 4G or 3G, over the corporately shared internet connection or over the OpenVPN which uses one of three fibre connections.
- 2.2. The quality of the connection will impact the successfulness of the meetings, regardless of what audio/video conferencing tool is used and is out of the control of ICT.
- 2.3. For information, ICT have completed a tendering process for a new shared internet connection which has been awarded to Virgin Media Ltd to provide a 200mb uncontended internet connection, this will eventually replace the existing shared 40mb uncontended internet connection. Once installed and configured

this should alleviate many connection issues into and out of the authority network. We are awaiting an installation date from Virgin.

- 2.4. We are also in the process of reviewing the most appropriate audio/video conferencing tool which will determine the most appropriate tool for the medium term.

2 Conclusions and Reasons for Recommendation

- 2.1 The use of audio and video conferencing tools are essential to effective day-to-day businesses of the council. This is certainly true whilst ever social distancing restrictions are in place but the likelihood is that it will become a fundamental business tool of the future.

The measures outlined in this report strike the balance between effective day-to-day business and mitigating risks as far as practicably possible.

Consultation and Equality Impact

- 3.1 Consultation has been previously sought with Senior Management and the Data Protection Officers at each authority.

4 Alternative Options and Reasons for Rejection

- 4.1 Do not accept the Risks and ICT do not allow the use of video conferencing tools to join meetings only allowing access to the current corporate software.
- 4.2 Make alternative recommendations to the protocol as deemed necessary.

5 Implications

5.1 Finance and Risk Implications

- 5.1.1 See **Appendix 5** – Audio and Video Conferencing risk Register 28.04.20
- 5.1.2 Risks of not participating in Official council meetings organised by third party organisations.

5.2 Legal Implications including Data Protection

- 5.2.1 The Data Protection Officer supports the issuing of protocols as an effective organisational measure to inform employees and Members on the use of audio and video conferencing tools and to reduce the risks noted on the specific risk assessment.
- 5.2.2 The Data Protection Officer has reviewed the protocols and given advice which has been incorporated into the documentation.
- 5.2.3 The Data Protection Officer has reviewed the risk assessment and considers that it accurately reflects the risks from a data protection perspective.

5.3 **Human Resources Implications**

- 5.3.1 Protocols are distributed to all Members and require acceptance before using Video and Audio conferencing tools.

6 **Recommendations**

- 6.1. That Joint ICT Committee support the adoption and acceptance of the Members Protocol for the use of Video and Audio Conferencing Tools to mitigate the risks with using Video and Audio Conferencing Tools.
- 6.2 That Joint ICT Committee acknowledge details of the report including associated risks and mitigation.

7 **Document Information**

Appendix No	Title
Appendix 5	Appendix 5 – Audio and Video Conferencing risk Register 28.04.20 *
Background Papers (These are unpublished works which have been relied on to a material extent when preparing the report. They must be listed in the section below. If the report is going to Cabinet (NEDDC) or Executive (BDC) you must provide copies of the background papers)	
Appendix 5 – Audio and Video Conferencing risk Register 28.04.20 * *The Members protocols are different for DDDC, BDC and NEDDC. Therefore the ‘Members Protocol for the use of Video and Audio Conferencing Tool’ for each authority has previously been sent separately via email to all members of that authority.	
Report Author	Contact Number
Nicola Astle, Joint ICT Service Delivery Manager	01246 217611

Risk Register Owner: Data Protection Officer NEDDC / BDC										DATE OF LAST REVIEW: 24/04/2020						
REF	STRATEGIC AIM <i>this impacts on</i>	RISK <i>What is the issue: what is the root cause/problem; what could go wrong</i>	CONSEQUENCE/EFFECT: <i>What would occur as a result, how much of a problem would it be ?, to whom and why</i>	EXISTING ACTIONS/CONTROLS	RESIDUAL RISK SCORE <i>(See Scoring Table for guidance)</i>			FURTHER MANAGEMENT ACTIONS/CONTROLS REQUIRED	TARGET RISK SCORE <i>(See Scoring Table for guidance)</i>			COST	RISK OWNER	RISK OWNER DEPARTMENT	TARGET DATE	
					IMPACT	LIKELIHOOD	RISK RATING (xL)		IMPACT	LIKELIHOOD	RISK RATING (xL)					
IG1		<p>System data is accessed by unauthorised persons and used or shared inappropriately.</p> <p>Prospect of 'Hacking' or unlawful access whilst using Audio and Video Conferencing apps such as GoToMeeting, Zoom, Skype, Micosfot Teams, Cisco Webex</p> <p>Risks to the individual as a result of contravention of their rights in relation to privacy, or loss, damage, misuse or abuse of their personal information.</p>	<p>~Risk of breach of GDPR principles (f) security and the Accountability principle.</p> <p>~Non-compliance with the DPA or other legislation can lead to sanctions and fines .</p> <p>~Data disclosed reported to media and regulatory bodies resulting in reputational damage</p>	<p>The preferred software provider GoToMeetings 90 trail for audio/Video Conferencing which has end to end encryption.</p> <p>Zoom - release AES 256 encryption on 23rd April, but requires v5 app download. Skype - Uses AES 256 encryption.</p>	5	4	20	<p>Protocols on using Audio and Video Conferencing for hosting GoToMeeting.</p> <p>~ Use of Passwords for meetings</p> <p>~Lock meetings/waiting rooms.</p> <p>~ File/ screen sharing restrictions</p> <p>Only paid accounts to be used to HOST meetings.</p>	5	3	15		SAMT	SAMT		
IG2		<p>Personal data actually disclosed to unauthorised indivudals due to home working environment</p> <p>Computer screens positioned in a way that personal data is visible to unauthorised persons e.g. through windows, family members. Inadequate disclosure controls increase the likelihood of information being shared inappropriately, resulting in potential harm and distress to the data subject.</p> <p>Personal data can be overheard by members of the family and neighbours Calls with inadequate disclosure controls increase the likelihood of information being shared inappropriately, resulting in potential harm and distress to the data subject.</p> <p>Surroundings are not secure with the risk that personal data is compromised e.g photos, paperwork visible on camera Visible documents, photos etc with inadequate disclosure controls increase the likelihood of information being shared inappropriately, resulting in potential harm and distress to the data subject.</p> <p>Recording devices such as Alexa may record information from in audio/video conferences resulting in unauthorised access to business information. Inadequate disclosure controls increase the likelihood of information being shared inappropriately, resulting in potential harm and distress to the data subject.</p>	<p>~Risk of breach of GDPR principles (f) security and the Accountability principle.</p> <p>~Non-compliance with the DPA or other legislation can lead to sanctions and fines .</p> <p>~Data disclosed reported to media and regulatory bodies resulting in reputational damage</p>	<p>No Policy or guidance to cover Audio and Video Conferencing</p> <p>Reliance on indivudals : ~ Positioning screens so that they cannot be seen through windows or where people can walk round the back. ~ Using headsets or headphones where possible. ~ Working in separate room from family - Closing doors and windows as appropriate. ~ Using the Blur background options or photo backgrounds.</p>	4	4	16	<p>~Protocol for the use of Video and Audio Conferencing Tools for Employees and Members covering: >Position screens so that they cannot be seen through windows or where people can walk round the back. >Work in separate room from family - Close doors and windows as appropriate >Use of the Blur background options or photo background used >Recording devices should be turned off/deactivated when undertaken audio or Video conferencing. Unless strictly necessary and participants have been informed by the host. >Use of headset or headphones.</p>	4	3	12		SAMT	SAMT		
IG3		<p>Personal Data being discussed in an insecure environment.</p> <p>Inadequate disclosure controls increase the likelihood of information being shared inappropriately, resulting in potential harm and distress to the data subject.</p> <p>Is this one in relation to an insecure technical environment?</p>	<p>Breach of Integrity and confidentiality principle Article 5 (1) (f) also Article 32 Security of Processing Financial and reputational damage. Enforcement action and possible fines from ICO</p>	<p>No controls currently in place as new process to assist with Covid 19.</p>	5	3	15	<p>~Protocol to users, clearly stating the personal data must not to discussed whilst using audio/video conferencing. Unless strictly necessary and guidance is included in the protocol to ensure that the identity of an individual is not revealed through the information provided e.g. use of scenarios,de-personalised references.</p>	5	2	10		SAMT	SAMT		

Risk Register Owner: Data Protection Officer NEDDC / BDC										DATE OF LAST REVIEW: 24/04/2020						
REF	STRATEGIC AIM <div>Page 36</div> this impacts on	RISK <div>What is the issue: what is the root cause/problem; what could go wrong</div>	CONSEQUENCE/EFFECT: <div>What would occur as a result, how much of a problem would it be ?, to whom and why</div>	EXISTING ACTIONS/CONTROLS	RESIDUAL RISK SCORE <div>(See Scoring Table for guidance)</div>			FURTHER MANAGEMENT ACTIONS/CONTROLS REQUIRED	TARGET RISK SCORE <div>(See Scoring Table for guidance)</div>			COST	RISK OWNER	RISK OWNER DEPARTMENT	TARGET DATE	
		IMPACT	LIKELIHOOD	RISK RATING (xL)	IMPACT	LIKELIHOOD	RISK RATING (xL)									
IG4		Third party Processor collects personal information about its users and doesn't provide a lot of detail about how it's used. Resulting in an individual's rights not being adhered to.	~Risk of breaching Chapter 3 of GDPR - individual's right to be informed ~Risk of breach or GDPR and corporate procedures on information security may result in financial and reputational damage. Enforcement action and possible fines from ICO	ICT Sign up to account T&C for GoToMeeting using provider T&Cs. There is no opportunity to alter or amend these T&C's if you don't sign up you cannot have the product.	5	4	20	~GoToMeetings - Only licensed individual able to host meetings. ~ ZOOM T&Cs are not clear – No one should be hosting meetings and no login details required or should be provided to Join the meetings. ~ Zoom app on Ipad does not require them to sign in.	5	3	15		SAMT	SAMT		
IG5		File Sharing – Facility allows for files to be uploaded and downloaded. Risk of malware being downloaded and compromising council networks resulting in harm and distress to individuals.	~Breach of Integrity and confidentiality principle Article 5 (1) (f) also Article 32 Security of Processing ~Financial and reputational damage. Enforcement action and possible fines from ICO	No controls currently in place as new process to assist with Covid 19.	5	5	25	~Guidance to employees informs them not to discuss personal data. ~Guidance to employees advising they should not download or upload Files via conference tools, use email, as filters and monitoring in place. Limited technical solutions can be put in place but only for pc's and laptops whilst on the network to prevent file sharing through conference tools. ~Monitoring guidance to Hosts to ensure no personal data discussed	5	4	20		SAMT	SAMT		

Risk Register Owner: Data Protection Officer NEDDC / BDC										DATE OF LAST REVIEW: 24/04/2020						
REF	STRATEGIC AIM <i>this impacts on</i>	RISK <i>What is the issue: what is the root cause/problem; what could go wrong</i>	CONSEQUENCE/EFFECT: <i>What would occur as a result, how much of a problem would it be ?, to whom and why</i>	EXISTING ACTIONS/CONTROLS	RESIDUAL RISK SCORE <i>(See Scoring Table for guidance)</i>			FURTHER MANAGEMENT ACTIONS/CONTROLS REQUIRED	TARGET RISK SCORE <i>(See Scoring Table for guidance)</i>			COST	RISK OWNER	RISK OWNER DEPARTMENT	TARGET DATE	
					IMPACT	LIKELIHOOD	RISK RATING (ixL)		IMPACT	LIKELIHOOD	RISK RATING (ixL)					
IG6		Video Conferencing recorded without the relevant privacy information being provided. Risk of breaching an individual's right to be informed	~Risk of breaching Chapter 3 of GDPR - individual's right to be informed ~Risk of breach or GDPR and corporate procedures on information security may result in financial and reputational damage. Enforcement action and possible fines from ICO	No controls currently in place as new process to assist with Covid 19.	3	3	9	Privacy notice to be prepared for meetings that are being recorded so that all participants are aware of how their information is being used. Or the protocols clearly advise that meeting participants needs to be informed in advance or at the beginning of the meeting if it is going to be recorded and why (its purpose) ~Hosting of meetings to only be done by corporately paid for accounts as recording can be restricted.	3	2	6		SAMT	SAMT		
IG7		The video conferencing recording retained for longer than necessary.	~Breach of Storage Limitation principle - GDPR Article 5 (1) (e) which may result in financial and reputational damage. Enforcement action and possible fines from ICO	~Record retention policy ~Information Asset Register	3	3	9	~Consideration that recordings of council meetings should be to Council devices and not stored in the cloud. Only Paid for GoToMeeting corporate accounts used for Hosting meetings which allows control over who can record meeting. ~Retention policies to be set and included on the Information Asset Register and Retention policy schedule. Protocol also notes that the recording needs to saved securely to the network and only saved for as long as it is needed for the purpose it was made.	3	3	9		SAMT	SAMT		

Risk Register Owner: Data Protection Officer NEDDC / BDC										DATE OF LAST REVIEW: 24/04/2020						
REF	STRATEGIC AIM this impacts on	RISK What is the issue: what is the root cause/problem; what could go wrong	CONSEQUENCE/EFFECT: What would occur as a result, how much of a problem would it be ?, to whom and why	EXISTING ACTIONS/CONTROLS	RESIDUAL RISK SCORE (See Scoring Table for guidance)			FURTHER MANAGEMENT ACTIONS/CONTROLS REQUIRED	TARGET RISK SCORE (See Scoring Table for guidance)			COST	RISK OWNER	RISK OWNER DEPARTMENT	TARGET DATE	
					IMPACT	LIKELIHOOD	RISK RATING (x4)		IMPACT	LIKELIHOOD	RISK RATING (x4)					
IG8	Page 38	Use of live streaming – video conferencing could be streamed live on Facebook/YouTube with out data subjects being give the appropriate privacy infomation.	~Risk of breaching Chapter 3 of GDPR - individual's right to be informed ~Risk of breach or GDPR and corporate procedures on information security may result in financial and reputational damage. Enforcement action and possible fines from ICO	~Policy for filming streaming council meetings.	3	3	9	~Restriction that only Public Council meetings would be streamed live. Agree. No change to current procedure. ~Include privacy information to participants	3	2	6		SAMT	SAMT		
IG9		Data centers for cloud based products are based outside of the UK and EU. Potential of access to data by counties such as China	Breach of Chapter V of GDPR International Transfer	~verbal instruction not to discuss personal data on audio/Video conferencing	5	4	20	GoToMeeting has GDPR compliant arrangements in place for data storage and transfer. '~ZOOM – Changes as of 18 April means that for paid accounts security allows enforcement through EU data Centers. Policy enforces only paid for accounts to HOST meetings. No controls when joining meetings. Protocol advises not to discuss anything official-sensitive when joining meetings.	5	3	15		SAMT	SAMT		
IG10		Video conferencing does not have end to end encryption which mean that there is a chance of the network being prone to cyber-attacks. Harm and distress to individuals	Breach of Integrity and confidentiality principle Article 5 (1) (f) also Article 32 Security of Processing Financial and reputational damage. Enforcement action and possible fines from ICO	~ GoToMeeting, which is the prefereed software, has ISO27001 acreditation and end to end encryption - as of 23rd april and v5 app - Zoom has AES 256 encryption. Skype - also has AES 256 encryption.	5	5	25	GoToMeeting had end to end encrytion.Latest version of Zoom has AES 256 Encrytion, until 1st June this may not be the case. '~ Protocol for Use of Audio and Video conferencing to be issued to all employees and members to reduce the risk of personal and sensitive information being compromised.	5	4	20		SAMT	SAMT		
IG11		Personal devices used to download apps for business use. No control over what devices are being used or how individuals have signed up for products. e.g using work email address to sign up for free trials	~Inadequate organisation and technical measures resulting in a potential breach of Integrity and confidentiality principle Article 5 (1) (f) also Article 32 Security of Processing ~Financial and reputational damage. Enforcement action and possible fines from ICO	ICT security policy advises that only corporate devices should be used, however some of the early communciations may have encouraged staff to use personal devices.	5	4	20	~Protocol to be issued to all employees on the use of audio and video conferencing which clearly states the Councils' preferred option and restricts other application unless authorised.. ~GoToMeeting – User guide and Host guide available.No file egress on gotomeeting and Corporately hosted accounts have the ability to record restricted where not required. ~Only corporately paid for accounts should organise meetings. Non organisers' should not and do not need to sign up. No technical controls available to prevent this.	5	3	15		SAMT	SAMT		
IG12		Risk of data being accidentally or deliberately compromised, cyber security issues Use of zoom which has reported poor security Harm and distress to individuals	~Breach of Integrity and confidentiality principle Article 5 (1) (f) also Article 32 Security of Processing ~ Financial and reputational damage. Enforcement action and possible fines from ICO	~GoToMeeting 90 day trial provided security assurances such as ISO27001 and end to end encryption. - Zoom now provides end to end encrytpion after 1st June	5	5	25	~Only corporately paid for accounts should organise meetings. Non organisers' should not and do not need to sign up. No technical controls available to prevent this but clearly noted in the protocols. ~Guidance to employees /Members advising they should not download or upload Files via conference tools, use email, as filters and monitoring in place ~Limited technical solutions can be put in place but only for pc's and laptops whilst on the network to prevent file sharing through conference tools.	5	4	20		SAMT	SAMT		
IG13		Risk of disruption to Public Council meetings. Harm and distress to individuals	~Reputational damage to the Council	~Host able to control who is in the meeting and remove anyone who causes a problem	3	3	9	~Only corporately paid for licences host council meetings and settings are set as per security guidance for the product. ~Use Protocol of Audio and Video Conferncing to be issued asGuidance ~meetings by invitation only with strong passwords set. Meetings locked once all participants are in.	3	2	6		SAMT	SAMT		
IG14							0				0					